iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43589

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Review Paper on Computer Network Security and Privacy

Ms. Smruti R. Mali[1], Ms. Amruta D. Patil[2], Prof. Mrs. K. N. Rode[3]
[1, 2]*Student, Dept. of E&TC, SITCOE, Yadrav, Maharashtra, India*
[3]*Mentor, Dept. of E&TC, SITCOE, Yadrav, Maharashtra, India*

Abstract: ***As the sizable recognition of laptop community applications, its safety is likewise acquired a excessive diploma of attention. Factors affecting the protection of community are complex. Network safety is a scientific paintings, has the excessive challenge. For protection and reliability troubles of laptop community gadget, this paper mixed with realistic paintings experience, from the risk of community safety, safety technology, community a few Suggestions and measures for the gadget layout principle, with a purpose to make the loads of customers in laptop networks to decorate protection attention and grasp positive community safety technology.***
Keywords: Network, Security; Technology, Strategies, Principle.

I. INTRODUCTION

Nowadays, the application of computer network has extended to every corner of the world and areas, is an unprecedented impact on people's work and life, as well as electric power, transportation, and has increasingly become an integral part of people's life. At the same time, with the expanding of network size, and the understanding of network knowledge is more and more in-depth, more and more unsafe factors such as the network attack, has been a serious threat to network and information security. Computer network security has become a global concern. Computer network and information security technology is the core issue of the computer and network systems foreffective protection. Network security. Protection involves very wide range, from a technical level, mainly including data encryption, identity authentication, intrusion detection and intrusion protection, virus protection and virtual private networks (VPNS), etc., some of these technologies is active defense, some of them are passive protection, and some are to provide support and platform for the research of security. Computer network security by adopting various technical and management measures make the normal operation of the network system, to ensure the availability, integrity and privacy of network data. So, to establish the purpose of network security protection is to

II. NETWORK SECURITY

Network protection consists of policies and configurations which might be made to defend the integrity, confidentiality and accessibility of pc networks and data. Network protection is designed to defend the usability and integrity of your community and data. It consists of each hardware and software program technologies. It goals lots of threats. It resists them from getting into or spreading to your community. Effective community protection manages get right of entry to the community. Every organization, irrespective of size, enterprise or infrastructure, calls for a diploma of community protection answers in vicinity to defend it from the ever-developing panorama of cyber threats within side the wild today.

Today's community structure is complicated and is confronted with danger surroundings this isusually converting and attackers which are usually attempting to find and make the most vulnerabilities. These vulnerabilities can exist in an extensive variety of areas, along with devices, data, programs, customers and locations. For this reason, there are numerous community protection control equipment and programs in use these days that cope with person threats and exploits and additionally regulatory non-compliance. When only some minutes of downtime can reason tremendous disruption and big harm to an organization's backside line and reputation, it's far vital that those safety measures are in proper place.

A. How Does Community Safety Work?

There are many layers to recall even as addressing network protection for the duration of an organization. Attacks can show up at any layer inside facet the network protection layers model, so your network protection hardware, software program software and regulations want to be designed to cope with each area. Network protection normally consists of three one in all a type controls: bodily, technical and administrative.

Here is a short description of the only of type forms of network protection and the manner each manages works.

1) Physical Network Security: Physical safety controls are designed to save you unauthorized employees from gaining bodily get entry to community additives together with routers, cabling cabinets and so on. Controlled get entry to, together with locks, biometric authentication and different devices, is crucial in any organization.
2) Technical Network Security: Technical safety controls shield statistics this is saved at the community or that's in transit across, into or out of the community. Protection is twofold; it desires to shield statistics and structures from unauthorized employees, and it additionally desires to shield towards malicious sports from employees.
3) Administrative Network Security: Administrative safety controls encompass safety rules and procedures that manage consumer behavior, along with how customers are authenticated, their stage of get entry to and additionally how IT personnel participants put into effect adjustments to the infrastructure.

B. How are we able to Make Sure Community Safety?

We have to make sure that the passwords are Strong and Complex everywhere- in the community too, now no longer simply on person computer systems inside an org. These passwords can't be easy, default and effortlessly guessable ones. This easy step can pass a protracted manner closer to securing your networks.

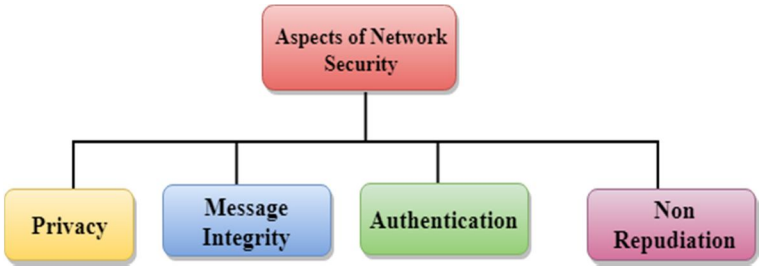
C. Why is Security so Important?

Information security performs key roles such as:

1) The organization's ability to function without any hindrance
2) Enabling the safe operation of applications implemented on the organizations IT systems
3) Protecting the data the organization collects and its uses

III. ASPECTS OF NETWORK SECURITY

Following are the suited residences to reap stable communication:



1) *Privacy:* Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
2) *Message Integrity:* Data integrity method that the statistics have to arrive on the receiver precisely because it become dispatched. There have to be no adjustments within side the statistics content material at some stage in transmission, both maliciously or accident, in a transit. As there are increasingly more financial exchanges over the internet, statistics integrity is greater crucial. The statistics integrity have to be preserved for stable communication.
3) *End-factor Authentication:* Authentication method that the receiver is certain of the senders identification, i.e., no imposter has dispatched the message.
4) *Non-Repudiation:* Non-Repudiation method that the receiver has to be capable of show that the obtained message has come from a particular sender. The sender has to now no longer deny sending a message that she or he send. The burden of proving the identification comes at the receiver. For example, if a consumer sends a request to switch the cash from one account to any other account, then the financial institution have to have a evidence that the consumer has asked for the transaction.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

IV. PRIVACY

The idea of the way to reap privateness has now no longer been modified for lots of years: the message can't be encrypted. The message has to be rendered as opaque to all of the unauthorized parties. A exact encryption/decryption method is used to reap privateness to a few extent. This method guarantees that the eavesdropper can't apprehend the contents of the message.

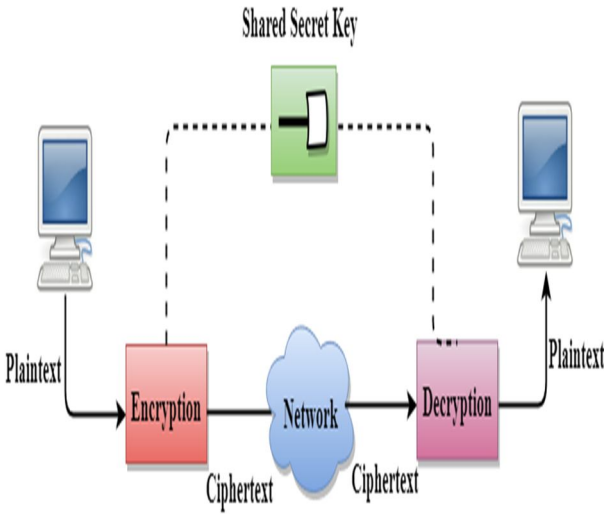
A. Encryption/Decryption

1) *Encryption:* Encryption method that the sender converts the authentic statistics into any other shape and sends the unintelligible message over the community.
2) *Decryption:* Decryption reverses the Encryption procedure on the way to remodel the message returned to the authentic shape. The statistics that's to be encrypted on the sender web.Web page is referred to as plaintext, and the encrypted statistics is referred to as cipher text. The statistics is decrypted on the receiver web page.

There are styles of Encryption/Decryption techniques:

- Privacy with mystery key Encryption/Decryption.
- Privacy with public key Encryption/Decryption.

B. Secret Key Encryption/Decryption Technique



1) In Secret Key Encryption/Decryption technique, the identical secret's utilized by each the events, i.e., the sender and receiver.
2) The sender makes use of the name of the game key and encryption set of rules to encrypt the data; the receiver makes use ofthis key and decryption set of rules to decrypt the data.
3) In Secret Key Encryption/Decryption technique, the set of rules used for encryption is the inverse of the set of rules used for decryption. It manner that if the encryption set of rules makes use of a aggregate of addition and multiplication, then the decryption set of rules makes use of a aggregate of subtraction and division.
4) The mystery key encryption set of rules is likewise referred to as symmetric encryption set of rules due to the fact the identical mystery secret's utilized in bidirectional communication.
5) In mystery key encryption/decryption set of rules, the name of the game code is utilized by the laptop to encrypt the records earlier than it's miles dispatched over the community to any other laptop.
6) The mystery key calls for that we need to realize which computer systems are speak me to every different in order that we will set up the important thing on every laptop.

C. Data Encryption Standard (DES)

- The Data Encryption Standard (DES) become designed with the aid of using IBM and followed with the aid of using the U.S. authorities as the usual encryption technique for nonmilitary and nonclassified use.
- The Data Encryption Standard is a widespread used for encryption, and it's miles a shape of Secret Key Cryptography.

1) Advantage

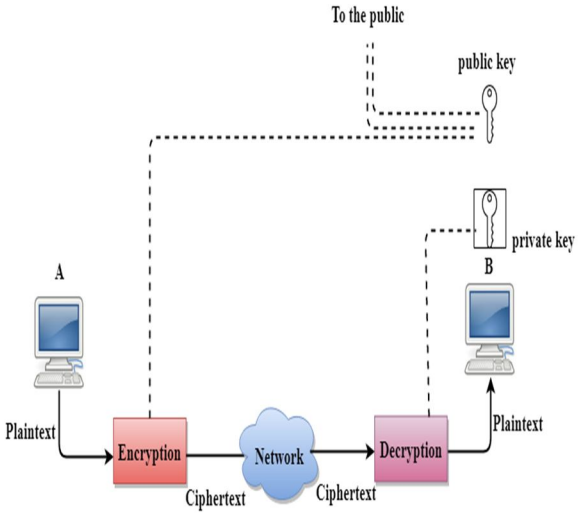
- *Efficient:* The mystery key algorithms are extra green because it takes much less time to encrypt the message than to encrypt the message with the aid of using the usage of a public key encryption set of rules. The motive for that is that the scale of the secret's small. Due to this motive, Secret Key Algorithms are specifically used for encryption and decryption.

2) Disadvantages

- The Secret Key Encryption/Decryption has the subsequent disadvantages:
- Each pair of customers need to have a mystery key. If the range of humans desires to use this technique withinside the international is N, then there are N(N-1)/2 mystery keys. For example, for 1,000,000 humans, then there are 1/2 of billion mystery keys.
- The distribution of keys amongst distinct events may be very difficult. This trouble may be resolved with the aid of using combining the Secret Key Encryption/Decryption with the Public Key Encryption/Decryption algorithm.

D. Public Key Encryption/Decryption Technique

- There are two keys in public key encryption: a private key and a public key.
- The private key is given to the receiver while the public key is provided to the public.



- In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.
- In public key Encryption/Decryption, the public key used by the sender is different from the private key used by the receiver.
- The public key is available to the public while the private key is kept by each individual.
- The most commonly used public key algorithm is known as RSA.

1) Advantages

- The fundamental restrict of private key encryption is the sharing of a thriller key. A 1/3 birthday party cannot use this key. In public key encryption, each entity creates more than one keys, and they hold the personal one and distribute the overall public key.
- The amount of keys in public key encryption is reduced tremendously. For example, for one million clients to communicate, handiest million keys are required, now not a half-billion keys as withinside the case of thriller key encryption.

2) Disadvantages

- *Speed:* One of the important downside of the general public-key encryption is that it`s miles slower than mystery-key encryption.In mystery key encryption, a unmarried shared secret is used to encrypt and decrypt the message which quickens the technique at the same time as in public key encryption, exceptional keys are used, each associated with every one-of-a-type thru a complicated mathematical technique.Therefore, we will say that encryption and decryption take extra time in public key encryption.
- *Authentication:* A public key encryption does now not have a integrated authentication. Without authentication, the message may be interpreted or intercepted without the user`s knowledge.
- *Inefficient:* The most important downside of the general public secret is its complexity.If we need the approach to be effective, huge numbers are needed.But in public key encryption, changing the plaintext into cipher text using extended keys takes some of time.Therefore, the general public key encryption algorithms are green for quick messages now not for extended messages

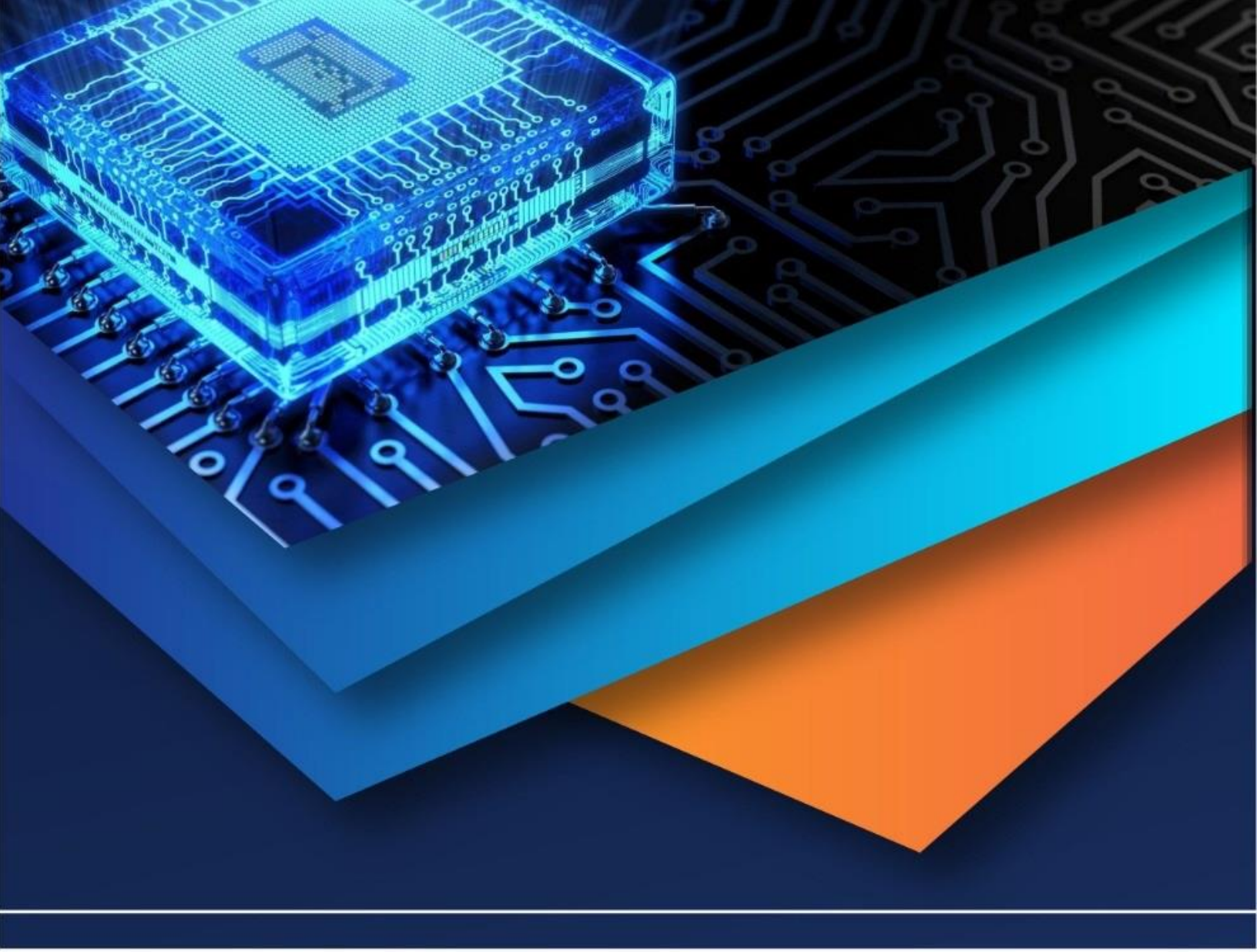
V. CONCLUSION

Internet property, email and therefore the net, currently important for little business, create several risks to laptop systems and therefore the privacy of the company's knowledge. The onslaught of viruses, worms, and Trojan horses, combined with the increasing drawback of spyware, adware, associate degreed integrated threats still attack an organization's network through multiple strategies.

Without effective network-defense and disaster-recovery practices a business is continually in danger. Defense needs regularly updated product like Symantec Antivirus or Symantec shopper Security, and a well-defined outbreak-response commit to establish and cope with this ever-expanding drawback. Symantec Antivirus and Symantec shopper Security offer a good barrier against security risks and threats, facilitating their identification and removal, and defend sensitive and personal company knowledge. while not this protection, corporations would possibly notice themselves round-faced with associate degree body nightmare, together with time intense and expensive full system reloads to recover lost knowledge.

REFERENCES

[1] https://www.javatpoint.com/computer-network-security
[2] https://ieeexplore.ieee.org/document/1556540
[3] https://www.tutorialspoint.com/data_communication_computer_network/computer_network_security.htm
[4] https://www.geeksforgeeks.org/network-security/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY